REMARKS

Reconsideration of the present application and entry of the present amendment are respectfully requested.

By means of the present amendment, the current Abstract has been amended as shown in the enclosed Replacement Abstract for better conformance to U.S. practice, where the last line referring to FIG. 5 has been deleted.

By means of the present amendment, the specification has been amended to improve form thereof, such as correcting a typographical error, deleting references to the claims, and adding reference numerals related to FIG 5.

In the Final Office Action, claims 1-6 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Without agreeing with the Examiner, and to advance prosecution and expedite allowance of the present application, claim 1 has been amended for clarification. Claim 1 was not amended in order to address issues of patentability and Applicant respectfully reserves all rights he may have under the Doctrine of Equivalents.

In the Final Office Action, claims 1, 3-4 and 7-8 were rejected under 35 U.S.C. §103(a) as being unpatentable over "The

Cipher SHARK" (Rijman) in view of "Function Hiding Based on Error Correcting Codes" (Loureiro). Further, claims 2 and 5 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rijman and Loureiro and further in view of "brute force" (FOLDOC). In addition, claim 5 was rejected under 35 U.S.C. §103(a) as being unpatentable over Rijman and Loureiro and further in view of "Multilevel Coded Modulation ..." (Isaka) and "Turbo Product Code Tutorial" (Williams).

Applicant respectfully traverses these rejections. However, to advance prosecution and expedite allowance of the present application, independent claim 1 has been amended to include a feature of dependent claim 6, which has been amended for conformance with amended claim 1. Accordingly, no new issues requiring a new search have been presented and thus entry of the present application is respectfully requested. It is respectfully submitted that claims 1-5 and 7-9 are patentable over Rijman, Loureiro, Isaka and Williams for at least the following reasons.

In rejecting claim 6, the Examiner correctly noted that Rijman, Loureiro, Isaka, and combination thereof do not teach or suggest shortening a code. Williams is cited in an attempt to

remedy this deficiency in Rijman, Loureiro, and Isaka.

While Williams teaches code shortening to enhance flexibility, there is simply no motivation to combine Williams with Rijman, Loureiro, Isaka, assuming arguendo that the combination of Rijman, Loureiro, and Isaka is proper. On page 7, last two lines of the Final Office Action, the reason given for such a combination is "shortening codes enhances flexibility." It is respectfully submitted that Rijman, Loureiro and Isaka are not concerned with enhancing flexibility; rather they are concerned with guaranteeing good diffusion, function hiding and unequal error protection, respectively, while concerns of the present application includes providing an invertible linear transformation for symmetric-key ciphers with optimal diffusion characteristics. It is respectfully submitted that such a combination of Rijman, Loureiro, Isaka and Williams can only be arrived using impermissible hindsight.

The prior art must be examined in light of the teachings of the prior art. The prior art may not be examined utilizing the teachings of the present application. There can be no suggestion or motivation to modify a reference if the proposed modification changes the principle of operation of the reference.

NL000444-aaf-10-3-05.doc   13

Applicant respectfully submits that present invention as recited in independent claim 1 can only be arrived using impermissible hindsight. There is nothing whatsoever in Rijman, Loureiro, Isaka and Williams, or combinations thereof, to suggest generating a code that is represented by a generator matrix including a matrix B, shortening this code, and then extending the matrix B, as recited in independent claim 1.

When Rijman, Loureiro, Isaka and Williams are reviewed without utilizing the teachings of the present application, then it is clear that Rijman, Loureiro, Isaka and Williams, and combinations thereof, do not disclose or suggest shortening the particular code which is generated by a generator matrix including a matrix B, and then extending the matrix B, as recited in independent claim 1. Without utilizing the teachings of the present application as a road map and hindsight reasoning, a person skilled in the art could not, in an obvious manner, arrive at the present invention as recited in independent claim 1.

In consideration of the use of improper hindsight for rendering a claim obvious in light of the prior art, the Federal Circuit has stated that "to draw on hindsight knowledge of the

patented invention, <u>when the prior art does not contain or suggest</u>

<u>that knowledge, is to use the invention as a template for its own</u>

<u>reconstruction - an illogical and inappropriate process by which to</u>

<u>determine patentability</u>." (Sensonics, Inc. v. Aerosonic Corp., 81

F.3d 1566, 38 USPQ2d 1551 (Fed. Cir. 1996). "<u>To imbue one of</u>

<u>ordinary skill in the art with knowledge of the invention ensued,</u>

<u>when no prior art reference or references of record convey or</u>

<u>suggest that knowledge, is to fall victim to the insidious effect</u>

<u>of a hindsight</u> syndrome wherein that which only the inventor taught

is used against its teacher." (In re Zurko, 111 F.3d 887, 42

USPQ2d 1476 (Fed. Cir. 1997). "A critical step in analyzing the

patentability of claims pursuant to section 103(a) is casting the

mind back to the time of invention, to consider the thinking of one

of ordinary skill in the art, <u>guided only by the prior art</u>

<u>references</u> and the then-accepted wisdom in the field (cited

reference omitted). <u>Close adherence to this methodology is</u>

<u>especially important in cases where the very ease with which the</u>

<u>invention can be understood may prompt one 'to fall victim to the</u>

<u>insidious effect of a hindsight</u> syndrome wherein that which only

the invention taught is used against its teacher (cited references

omitted).'" (In re Kotzab, 208 F.3d 1352, 54 USPQ2d 1308 (Fed. Cir. 2000). (Emphasis added)

In rejecting claims under 35 U.S.C. § 103, the Examiner bears the initial burden of establishing a prima facie case of obviousness. In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1442, 1444 (Fed. Cir. 1992). See also In re Piasecki, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984). The Examiner can satisfy this burden by showing that some objective teaching in the prior art of knowledge generally available to one of ordinary skill in the art suggests the claimed subject matter. In re Fine, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

When determining obviousness, "[t]he factual inquiry whether to combine references must be thorough and searching." In re Lee, 277 f.3d 1338, 1343, 61 USPQ 1430, 1433 (Fed. Cir. 2002), citing McGinley v. Franklin Sports, Inc., 262 F.3d 1339, 1351-52, 60 USPQ2d 1001, 1008 (Fed. Cir. 2001). "It must be based on objective evidence of record." Id. "Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence.'" In re Dembiczak, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617. "Mere denials and conclusory statements, however, are not

sufficient to establish a genuine issue of material fact."

Dembiczak, 175 F.3d at 1000, 50 USPQ2d at 1617, citing McElmurry v.

Ark. Power & Light Co., 995 F.2d 1576, 1578, 27 USPQ2d 1129, 1131

(Fed. Cir. 1993).

The suggestion in the Final Office Action that the

combinations of prior art references would be obvious to one having

ordinary skill in the art is respectfully refuted. One may not

utilize the teachings of the present application as a road map to

pick and choose amongst prior art references for the purposes of

attempting to arrive at the presently disclosed invention. The

Federal Circuit has identified three possible sources for

motivation to combine references including the nature of the

problem to be solved, the teachings of the prior art, and the

knowledge of persons of ordinary skill in the art. (See, In re

Rouffet, U. S. Court of Appeals Federal Circuit, U.S.P.Q. 2d, 1453,

1458.) There must be a specific principle that would motivate a

skilled artisan, with no knowledge of the present invention, to

combine the prior art as suggested in the Office Action. The use

of hindsight in the selection of references is forbidden in

comprising the case of obviousness. Lacking a motivation to

combine references, a proper case of obviousness is not shown (see,

In re Rouffet, 1458).

The U.S. Court of Appeals for the Federal Circuit (the

"Federal Circuit") restated the legal test applicable to rejections

under 35 U.S.C. § 103(a) in the In re Rouffet, holding. The Court

stated:

> [V]irtually all [inventions] are combinations of
> old elements. Therefore an Examiner may often
> find every element of a claimed invention in the
> prior art. Furthermore, rejecting patents solely
> by finding prior art corollaries for the claimed
> elements would permit an Examiner to use the
> claimed invention itself as a blueprint for
> piecing together elements in the prior art to
> defeat the patentability of the claimed
> invention. Such an approach would be "an
> illogical and inappropriate process by which to
> determine patentability." To prevent the use of
> hindsight based on the invention to defeat
> patentability of the invention, this court
> requires the Examiner to show a motivation to
> combine the references that create the case of
> obviousness. The Board [of Appeals] did not,
> however, explain what specific understanding or
> technological principle within the knowledge of
> one of ordinary skill in the art would have
> suggested the combination. ... To counter this
> potential weakness in the obviousness construct
> the suggestion to combine requirements stands as
> a critical safeguard against hindsight analysis
> and rote application of the legal test for
> obviousness. In re Rouffet, 47 USPQ2d 1457-58
> (Fed. Cir., July 15, 1998) (citations omitted).

More recently, the Federal Circuit again dealt with what is required to show a motivation to combine references under 35 U.S.C. § 103(a). In this case the court reversed the decision of the Board of appeals stating:

> [R]ather then pointing to specific information in Holiday or Shapiro that suggest the combination..., the Board instead described in detail the similarities between the Holiday and Shapiro references and the claimed invention, noting that one reference or the other-in combination with each other... described all of the limitations of the pending claims. Nowhere does the Board particularly identify any suggestion, teaching, or motivation to combine the ... references, nor does the Board make specific-or even inferential-findings concerning the identification of the relevant art, the level of ordinary skill in the art, the nature of the problem to be solved, or any factual findings that might serve to support a proper obviousness analysis. In re Dembiczak, 50 USPQ2d 1614, 1618 (Fed. Cir., April 28, 1999) (citations omitted).

Thus, from both In re Rouffet and In re Dembiczak it is clear that the Federal Circuit requires a specific identification of a suggestion, motivation, or teaching why one of ordinary skill in the art would have been motivated to select the references and combine them.

Thus, Applicant again respectfully submits that the Examiner

has used impermissible hindsight to reject claims 1-8 under 35

U.S.C. § 103(a). As discussed above, the Federal Circuit, in In re

Rouffet, stated that virtually all inventions are combinations of

old elements. Therefore an Examiner may often find every element

of a claimed invention in the prior art. To prevent the use of

hindsight based on the invention to defeat patentability of the

invention, the Examiner is required to show a motivation to combine

the references that create the case of obviousness. Applicant

respectfully submits that the Examiner has not met this burden.

The mere fact that the prior art device could be modified so

as to produce the claimed device is not a basis for an obviousness

rejection unless the prior art suggested the desirability of the

modification. See, In re Gordon, 733 F.2d 900, 902 (Fed, Cir.

1984); and In re Laskowski, 871 F.2d 115, 117 (Fed. Cir. 1989).

The only suggestion that can be found anywhere for making

these combinations appears to come from the present patent

application itself. How can the Final Office Action espouse that

this reconstruction of the present invention does not include

knowledge gleamed only from the applicant's disclosure? If this

reconstruction did not come from the present application, then

where did it come from? The above reconstruction certainly did not

come from the prior art.

Applicant respectfully maintains that there is no suggestion

in the prior art references to make the combinations in the manner

proposed by the Examiner to achieve the Applicant's claimed

invention.

The Examiner is requested to consider MPEP 2143, wherein it is

stated:

> THE PRIOR ART MUST SUGGEST THE DESIRABILITY OF
> THE CLAIMED INVENTION ... The teaching or
> suggestion to make the claimed combination and
> the reasonable expectation of success must both
> be found in the prior art, not in applicant's
> disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d
> 1438 (Fed. Cir. 1991)." And, "FACT THAT
> REFERENCES CAN BE COMBINED OR MODIFIED IS NOT
> SUFFICIENT TO ESTABLISH PRIMA FACIE OBVIOUSNESS
> ... The mere fact that references can be combined
> or modified does not render the resultant
> combination obvious unless the prior art also
> suggests the desirability of the combination. In
> re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir.
> 1990)... Although a prior art device "may be
> capable of being modified to run the way the
> apparatus is claimed, there must be a suggestion
> or motivation in the reference to do so." 916
> F.2d at 682, 16 USPQ2d at 1432.).

It is respectfully submitted that in light of the state of the

law as set forth by the Federal Circuit, that there is no proper

motivation for combining Rijman, Loureiro, Isaka and Williams to arrive to the present inventions as recited in amended independent claim 1.

Based on the arguments provided above, it is respectfully submitted that independent claim 1 is allowable, and allowance thereof is respectfully requested. In addition, it is respectfully submitted that claims 2-8 should also be allowed at least based on their dependence from independent claim 1.
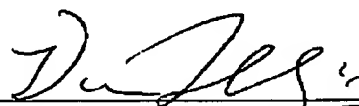
In addition, Applicant denies any statement, position or averment of the Examiner that is not specifically addressed by the foregoing argument and response. Any rejections and/or points of argument not addressed would appear to be moot in view of the presented remarks. However, the Applicant reserves the right to submit further arguments in support of the above stated position, should that become necessary. No arguments are waived and none of the Examiner's statements are conceded.

In view of the above, it is respectfully submitted that the present application is in condition for allowance, and a Notice of Allowance is earnestly solicited.

NL000444-aaf-10-3-05.doc   22

It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required for entrance of the accompanying amendment, they may be charged to applicant's representatives Deposit Account No. 50-3649. In addition, please credit any overpayments related to any fees paid in connection with the accompanying amendment to Deposit Account No. 50-3649.

Respectfully submitted,

By _____
Dicran Halajian, Reg. 39,703
Attorney for Applicant(s)
October 3, 2005

Enclosure: Replacement Abstract

THORNE & HALAJIAN, LLP
Applied Technology Center
111 West Main Street
Bay Shore, NY 11706
Tel: (631) 665-5139
Fax: (631) 665-5101

Replacement Abstract

A method of generating a linear transformation matrix A for use in a symmetric-key cipher includes generating a binary $[n,k,d]$ error-correcting code, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code. The code is represented by a generator matrix $G \in Z_2^{k \times n}$ in a standard form $G = (I_k \;||\; B)$, with $B \in Z_2^{k \times (n-k)}$. The matrix B is extended with $2k-n$ columns such that a resulting matrix C is non-singular. The linear transformation matrix A is derived from matrix C. Preferably, the error correcting code is based on an XBCH code.

~~FIG. 5.~~